Towards an Innovative Systemic Approach of Risk Management

Cholez, Hervé; Feltus, Christophe

DOI:
10.1145/2659651.2659734

Publication date:
2014

Document Version
Early version, also known as pre-print

Towards an Innovative Systemic Approach of Risk Management

Hervé Cholez and Christophe Feltus
Public Research Centre Henri Tudor,
29, avenue John F. Kennedy, L-1855 Luxembourg-Kirchberg, Luxembourg
herve.cholez@tudor.lu, christophe.feltus@tudor.lu

ABSTRACT

Nowadays, enterprises from different sectors are strongly interconnected and need to interact continuously in order to survive. In this context, the happening of an event (e.g., system failure) in one sector may lead to a serious risk in another. To avoid this, a systemic approach for risk management is required. This approach pursues the objective to foster the accuracy and the reactivity of the risk mitigation and hence minimize the impact and the propagation of the risk and, as a consequence, sustain the initiatives from all economic domains' regulators in risk management. This position paper suggests an innovative solution, which is to be further investigated, to manage cross-sector ICT ecosystem risks using enterprise architecture model. This solution is illustrated with a proof of concept related to the Luxembourgish market.

Categories and Subject Descriptors

H.2.7: Security, Integrity, and Protection

General Terms

Management, Performance, Design, Experimentation, Security, Languages, Theory, Verification.

Keywords

Information system, information security risk, systemic risk management, enterprise architecture, ArchiMate®, position paper.

1 INTRODUCTION & MOTIVATION

1.1 Context

Information systems are everywhere and their roles are central for all enterprises because of the increasing amount of information managed during the last decades. Due to the criticality of the information exchanged, more and more supervision is needed and operated by national, European or even international authorities. One of the leading sector having adopted such a model is the financial sector, with a national regulatory authority (NRA) established in every country and dealing with sector-based regulations, defined at the international and/or national level (e.g., Basel II agreements [1], the Sarbanes-Oxley Act [2], etc.)

The Luxembourgish market is based on a complex and integrated ecosystem and sustained by an integrated subcontractors network, especially in IT services. At the national level, the landscape of regulators to ensure the control of risks of different actors in the ecosystem is increasing, e.g., ILR[1] for the telecommunications service providers, ILNAS[2] for electronic records, CSSF[3] for the financial service providers, or the CNPD[4] for the data protection. These regulatory initiatives progressively allow improving the maturity of each actor and collecting data on related risks. However, due to the complexity and the heterogeneity of the market, the data analysis performed by the regulators, as well as the systemic risk management regarding this complete ecosystem remains challenging.

In this context, this position paper introduces, and gives an insight, to the research work that we are going to achieve in order to tackle the above systemic risks issue which we consider as the risk generated through the interaction between enterprises, having an influence on the whole customers'-/suppliers' chain, and impacting on more than one sector at the same time. This research work is founded by the Feder project named *SARIM* (Systemic Approach of Risk Management) and supported by a strong Luxembourgish partnership, as illustrated in Figure 1. The political level (european and national) establish laws and regulations. Partners on this level are, among others, the Ministry of State, the Ministry of Trade and Industry and the High Commissioner for National Protection. The national regulatory environment supervises the application of these regulations in the Luxembourgish organizations and their subcontractors. Partners in this sector are, among others: ILNAS, CNPD and ILR. Finally, ICT enablers, such as our partners of this project (EBRC (http://www.ebrc.com/), Post (http://www.post.lu), etc.), are essential to sustain the implementation of all these regulations and are also impacted by the regulatory environment.

1.2 Preliminary work

Before adressing an integrated ecosystem such as explained in the introduction, the Public Research Centre Henri Tudor experienced a two-years research project on one specific context: the telecommunications regulation [3]. In this project, conducted in collaboration with telecommunication operators and the ILR, the information security risk management (ISRM) process was an essential step and a strategic challenge.

SIN '14 , Sep 09-11 2014, Glasgow, Scotland Uk
ACM 978-1-4503-3033-6/14/09.
http://dx.doi.org/10.1145/2659651.2659734

[1] ILR ("Institut Luxembourgeois de Régulation") is the French acronym for Luxembourgish Regulatory Institute.

[2] ILNAS ("Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et qualité des produits et services") is the French acronym for Luxembourgish Institute for Standardisation, Certification, Security and Quality of Products and Services".

[3] CSSF ("Commission de Surveillance du Secteur Financier") is the French acronym for the Financial Services Authority.

[4] CNPD ("Commission Nationale pour la Protection des Données") is the French acronym for the national commission for data protection.

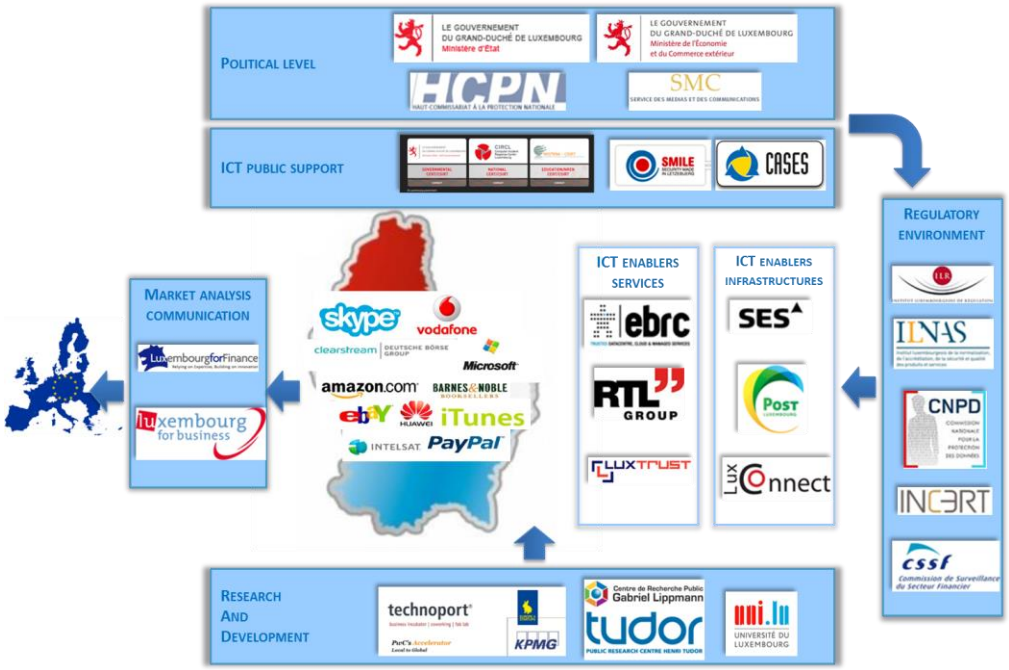

Figure 1. Integrated ecosystem of the Luxembourg digital economy governance

The project's key issues consisted in defining the relevant risks regarding the businesses operated and the architecture in place, as well as in selecting the relevant security controls accordingly.

As a result, the main innovation of this project consisted in the development of a specific ISRM process tailored to the telecommunication sector. The outcome of this project is a fine-tuned method supported by a tool (the TISRIM Telco Tool) which allows telecommunication operators to efficiently perform information security risk assessments in compliance with both national and European regulations.

The tool is distributed to all telecommunication operators in Luxembourg. Its large exploitation in Luxembourg allows a homogeneous methodology, and risk assessment results are easy to compare and to analyse by national regulatory authorities. Widespread implementation of risk assessment and security measures in this sector have positive benefits for both, citizens and the economy [3], as telecommunication networks will be better protected against service interruptions and security breaches, ensuring continuous and high-quality service. The TISRIM Telco tool helps the national regulatory authority to raise awareness of telecommunication operators, as well as to encourage the ongoing improvement of their level of information security.

This challenge of adapting information security risk management processes and practices to the telecommunication sector has strengthened our competencies in the domain. The large success of this project and the demands of the market have encouraged us to consider the developed materials in order to deploy the same approach in other sectors. This previous project was a first step that enabled an extremely challenging work on national governance of systemic risks with all main regulators. Based on this experience, we aim to develop an innovative systemic approach of risk management dedicated to the complex and integrated Luxembourgish market's ecosystem.

The next section describes our objectives and the research method to ellaborate this project.

2 FORESEE RESEARCH

2.1 Objectives

The objectives of this position paper are the definition of a common security risk management framework shared between all actors of the different sectors. This framework aims at bringing together the regulated enterprises for elaborating (1) a systemic risk management approach tailored to IT service systems and compliant to the Luxembourgish context and standards, (2) a risk management interface allowing agreements between actors and easing the service level agreement management, and (3) a method for monitoring risks at the national level.

As a result, this framework also sustains the regulators' activities by offering:

- an overview of the players and an identification of the service systems following an enterprise architecture approach in network;
- a set of models dedicated to the different sectors (business models, information system models, infrastruture models, etc.);
- a method for the analysis and the interoperability of the data collected by the regulators.

2.2 Research method

The research method for elaborating the cross-sector risk management framework consists of four phases: (1) definition of scope and requirements, (2) cross-sector interaction and risk modelling, (3) deployment and exploitation framework, (4) professional dissemination.

Definition of scope and requirements. The first phase aims at depicting the scientific literature related to the systemic approach and interoperability for risk management as well as of languages and models proposed for the formalisation of the method.

Cross-sector interaction and risk modelling. The second phase has as objective to define, a set of conceptual models sustaining the risk management, the systemic risk management and the sectorial risk management based on the review of the literature. In

that perspective we have decided to exploit enterprise architecture theory, i.e. ArchiMate. This phase constitutes the core of the research and is therefore detailed in the next section.

Deployment and exploitation framework. The third phase aims at developing tools based on previous models to bring to the regulated enterprises to perform a systemic risk management. We also deploy a specific regulator package to exploit the models elaborated in previous phases by considering the aspects of risk mapping, risk ecosystem, and risk interface.

Professional validation and dissemination. The fourth phase of the research is dedicated to an *in situ* experimentation followed by sectorial dissemination.

In the next section, we explain the approach that we propose. Therefore, we first present ArchiMate and then introduce an integrated map of the main components of the approach.

3 PROPOSED APPROACH

3.1 ArchiMate

ArchiMate [4] is an enterprise architecture [5] modelling language supported by The Open Group and aiming at modelling all concepts that compose an enterprise information system (IS). ArchiMate is especially dedicated to enterprises which are organised following a service based approach. It structures the enterprises' concepts following three layers (Figure 2): business, application, and technology according to three dimensions: information, behaviour, and structure. The language is composed of a set of core concepts and of two extensions: the motivation extension and the migration extension which respectively aims at modelling the reasons that underlay the design or change of some enterprise architectures and to provide concepts to support the implementation and migration of architectures. In addition, two extension mechanisms allow defining new concepts of the core and the extension models: the addition of attribute(s) and the creation of stereotype(s). For instance, these extension mechanisms have been used, e.g., to define a security extension aiming at analysing and mitigating the IS risk [6].

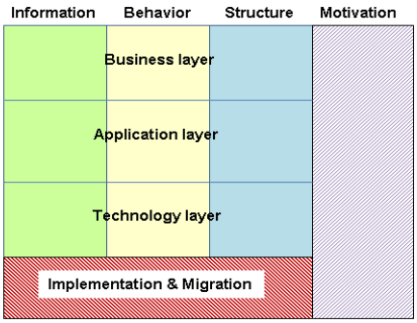

Figure 2. ArchiMate metamodel

The objectives of enterprise architecture models are various. The most important is that they allow illustrating the interconnections between the concepts that compose the enterprise architecture and hence the impact a modification of one concept has on the other, for instance, the impact of a server failure on a business service. Another objective is the definition of specific views on different aspects of the architecture depending on the different application required. For instance, the language may be used to extract a view only dedicated to the business aspects of the enterprise, a view related to a specific service, or a view related to the management of the security [6].

3.2 Cross-sector interaction and risk modelling approach

As explained in the introduction, enterprises from different fields are strongly interconnected and nowadays, a risk happening in one business sector is very likely to have an impact on other sectors. Unfortunately, information exchange among different sectors is limited which makes it sometimes difficult to efficiently share appropriate and crucial information regarding systemic security. As explained in the research method, one of the first steps is to develop cross-sector interaction and risk modelling, in particular by developing conceptual models allowing describing the ecosystem and the different interactions.

As a result, our approach to face this problem consists of using and adapting an existing and well established enterprise architecture language which allows modelling all the sector characteristics. Figure 3 represents the different dimensions of our approach in a UML like language. In this figure, we note that enterprises from different sectors often need to interact in order to achieve specific goals. E.g., in order to regulate the activities and to improve the quality of the services provided by an enterprise in the financial sector, the regulatory authorities require performing an appropriate risk management activity. To have this high quality risk management activity generate accurate results, different interactions with other sectors also need to be taken into account. For instance, this financial enterprise needs to use highly available networks provided by telecommunication operators and, as a result, appropriate information should be exchanged between these enterprises.

In this context, to sustain this risk management, it is necessary to represent the following elements through a single enterprise architecture modelling language (ArchiMate): enterprise IS, risk management, interaction between enterprises, and risk management related to this interaction. Using a single language for representing heterogeneous information issued from different domains allow these different enterprises to more easily access and understand the semantic of the systemic risks and to facilitate the exchange of information.

Figure 3 also represents the ISRM model of the whole Luxembourgish ecosystem. Several regulatory authorities regulate enterprises of different economic sectors. All of these enterprises have different goals but, however, need to interact. A risk management is commonly defined only in the scope of one enterprise. The main challenge is to take into account the enterprise's interaction to obtain a systemic risk management.

To address this type of risk management, we have exploited the ISRM model [7, 8] which proposes a risk management framework based on an extended and motivated risk management literature review. As explained in the window of figure 3 "Risk management based on ISRM", this risk model is composed of an event and one or more impacts on the enterprise goals. The event is itself composed of a threat that exploits one or more vulnerabilities of the enterprise's assets. However, as explained previously, the IS risk may have interdependencies between enterprises and should be related to the enterprise itself or to an interaction between enterprises.

Afterwards, to extend the risk management to an ecosystem management, we consider (1) the "Sectors based Risk management" as an instance of a more "traditional" IS risk management, and (2) the "Systemic risk management" (both dashed boxes of Figure 3). Our proposed research work consists in developing a set of conceptual models sustaining sectorial risk management and systemic risk management.

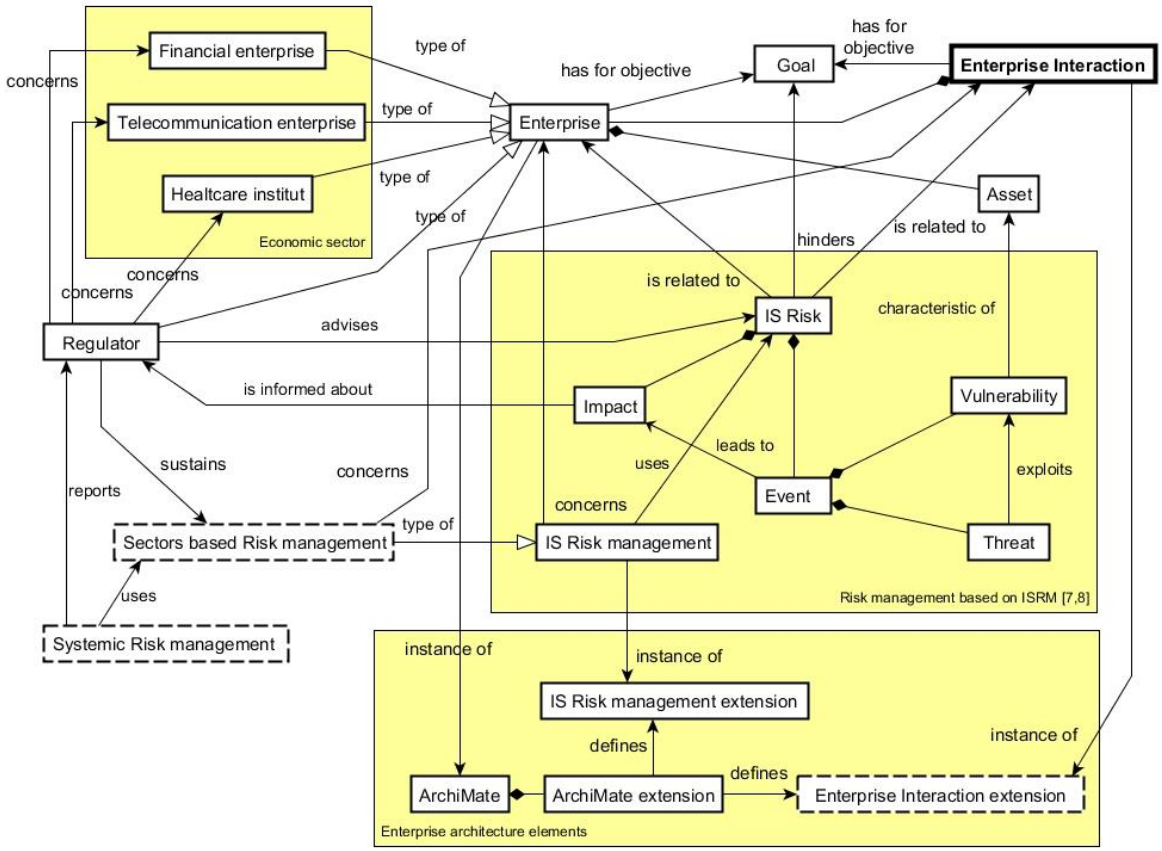

Figure 3. Foresee approach for cross-sector risk management

The last field according to our approach is the enterprise architecture. As illustrated at the bottom of Figure 3, the enterprise architecture models are perceived as appropriate solutions to sustain the modelling of the whole ecosystem (i.e., enterprises, interactions, and risk management). ArchiMate is a language with many advantages but we acknowledge that it is semantically not rich enough to model all the elements of the ecosystem, such as the Enterprise Interaction extension (dashed box). Enriching the ArchiMate language by using the extension mechanisms presented in previous sections is a key step of our approach.

This model is the first step of our work and illustrates the next main steps of this project by three challenge boxes (dashed boxes): the "sectors-based risk management modelling", the "enterprise interaction extension modelling", and the "systemic risk management framework".

4 CONCLUSIONS AND FUTURE WORKS

In this position paper, we have presented our approach to establish a systemic risk management framework. After having detailed our context and our preliminary work, we have exposed our foresee research with our different objectives and our research method. This framework will bring a systemic risk management approach tailored to service systems and compliant with the Luxembourgish context and standards to the regulated enterprises. This framework will also sustain the regulators' activities by offering a method for the analysis and the interoperability of the data collected by the regulators.

We have described our first step by modelling the systemic risk management in cross-sector interactions. Regarding future works, we have different challenging steps in the project: (1) the scope of the market and analysis of requirements, (2) the cross-sector interaction and risk modelling, (3) the deployment and exploitation framework, (4) the professional dissemination.

References

[1] Basel II. 2006. Bank for International Settlements BIS: International Convergence of Capital Measurement and Capital Standards: Revised Framework – Comprehensive Version.

[2] Sarbanes, P. S. and Oxley, M. 2002. "Sarbanes-Oxley Act of 2002".

[3] Mayer, N.; Aubert, J.; Cholez, H.; Grandry, E. 2013. Sector-Based Improvement of the Information Security Risk Management Process in the Context of Telecommunications Regulation, 20th European Conference, EuroSPI 2013, Dundalk, Ireland. Proceedings.

[4] Lankhorst, M. 2004. *ArchiMate* language primer, 2004.

[5] Zachman, J. A. 2003. The Zachman Framework For Enterprise Architecture : Primer for Enterprise Engineering and Manufacturing By. Engineering, no. July: 1-11.

[6] Grandry, E.; Feltus, C.; Dubois, E. 2013. Conceptual Integration of Enterprise Architecture Management and Security Risk Management, SoEA4EE'2013, Vancouver, BC, Canada.

[7] Mayer, N. 2009. Model-based management of information system security risk. PhD Thesis.

[8] Dubois, E.; Heymans, P.; Mayer, N. and Matulevičius, R. 2010. "A Systematic Approach to Define the Domain of Information System Security Risk Management," in *Intentional Perspectives on Information Systems Engineering*, Springer Berlin Heidelberg, pp. 289–306.